D-Link
Building Networks for People

Les réseaux sans fil & La sécurité, problématiques actuelles des entreprises et collectivités

Wi Fi™
The Standard for Wireless Fidelity

Yves REMY
Support Technique
D-Link France

Les différents réseaux sans fil

- **WPAN** : Wireless Personal Area Networks
  Réseaux sans fil de faible portée (quelques dizaines de mètres) qui sont des réseaux à usage personnel.

- **WLAN** : Wireless Lan Area Networks
  Réseau à plus large portée (une centaine de mètres) permettant d'interconnecter plusieurs utilisateurs. Equivalent du 802.3 filaire.

- **WMAN** : Wireless Metropolitan Area Networks
  Réseau permettant de relier les opérateurs de téléphonie à leurs clients sur une distance de 4 à 10 kilomètres. Boucle Locale Radio

- **WWAN** : Wireless Wide Area Networks
  Réseaux sans fil les plus utilisés aujourd'hui. GSM, GPRS et UMTS

Les normes de transmission

- Les normes 802.11 propres aux réseau Ethernet sans fils sont édictées par l'IEEE(Institute of Electrical and Electronics Engineers).

- Ils autorisent dans la bande des 2.4Ghz avec des puissances d'émission de 10 à 100mw selon les canaux des <u>débits théoriques maximum:</u>

→ de 11 Mbps en 802.11b.
→ de 54 Mbps en 802.11g.

- Le 802.11a opère dans la bande des 5Ghz avec un débit jusqu'à 54 Mbps.

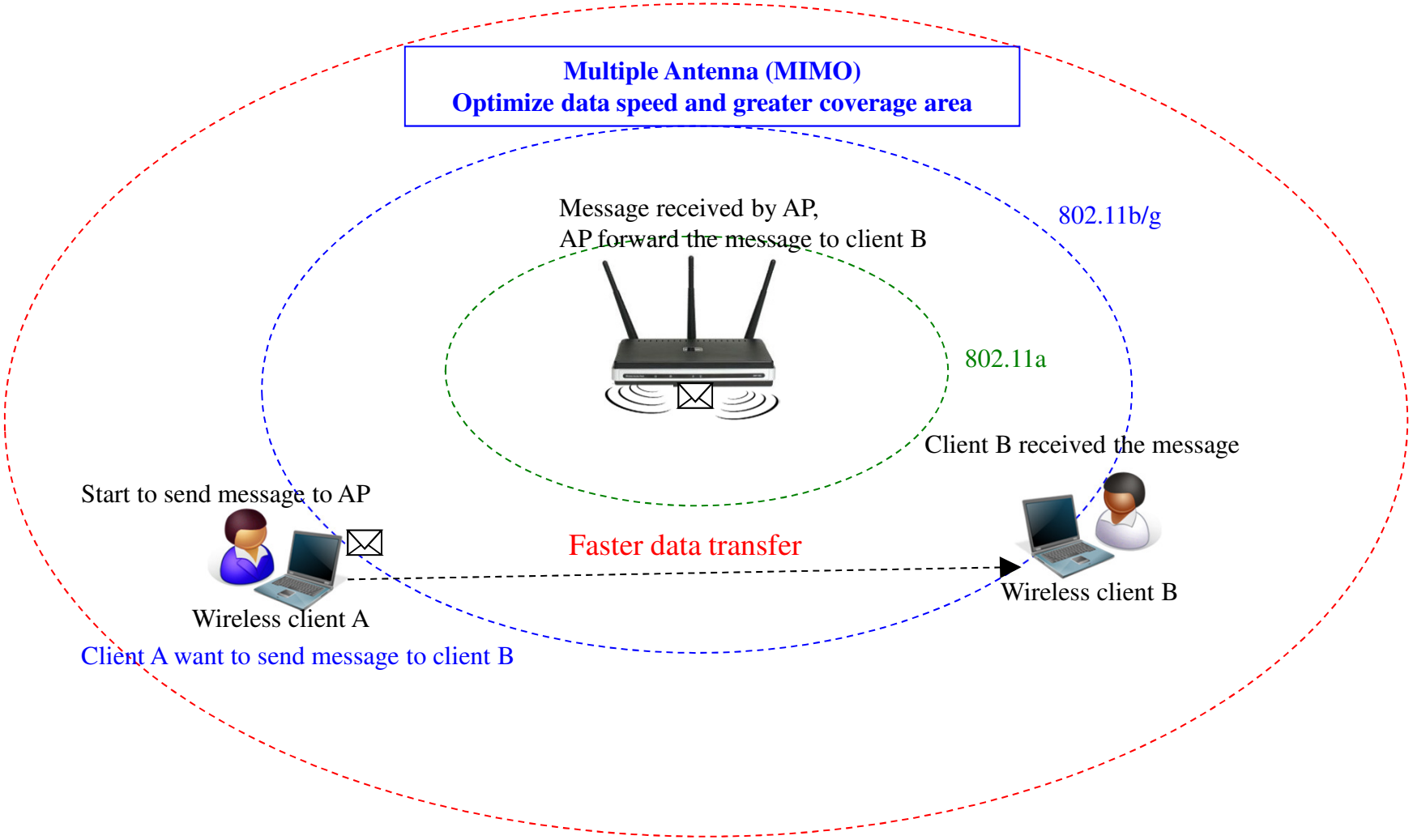
Les normes de transmission

Tableau récapitulatif des normes de transmission

	802.11b	802.11g	802.11a	802.11n
Fréquence	2.4Ghz	2.4Ghz	5Ghz	2.4Ghz-5Ghz
Bande de Fréquences	2,4-2,4835Ghz	2,4-2,4835Ghz	5,150-5,725Ghz	2.4 GHz, 5 GHz, 2.4 ou 5 GHz (sélectionnable), ou 2.4 et 5 GHz (simultané)
Les débits	11 Mbits/s théorique	54 Mbits/s théorique	54 Mbits/s théorique	300 Mbits/s théorique
Nombre de Bandes de fréquences (canaux)	13	13	19	
Le nombre de bandes de fréquences sans recouvrement	3	3	8	8
compatibilité	aucune	802.11b	aucune	802.11b,g,a

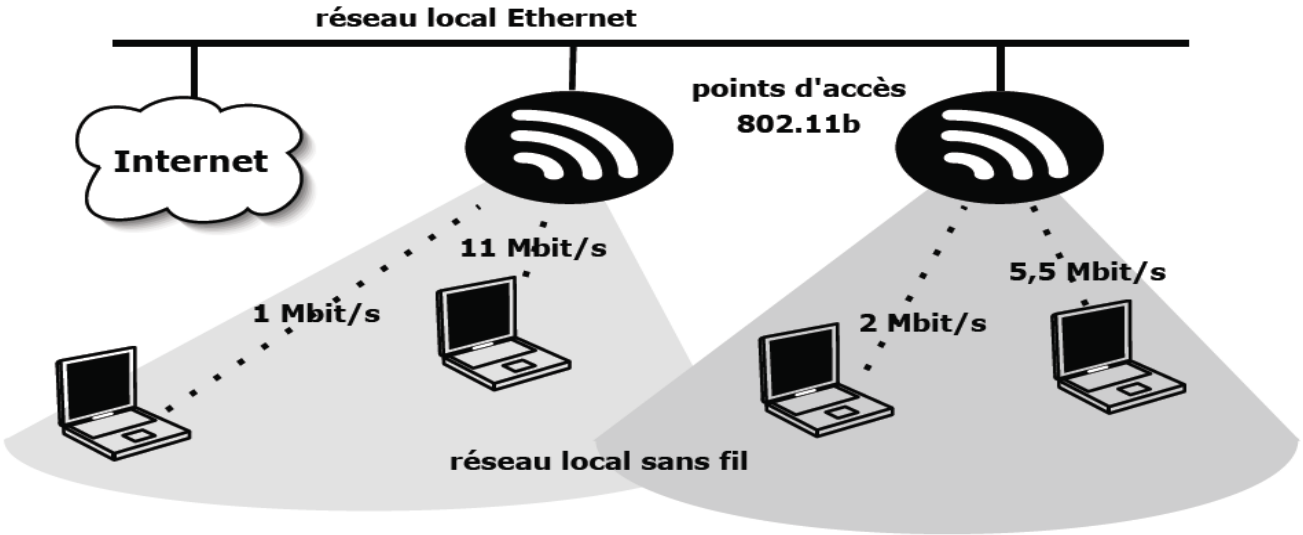
Les lois de la radio

Débit plus grand	**= Couverture plus faible**
Puissance d'émission élevée	**= Couverture plus grande, mais durée de vie des batteries plus faible**
Fréquences radio élevées	**= Meilleur débit, + sensible aux obstacles.** **=> couverture plus faible**


Multiple Antenna (MIMO)
Optimize data speed and greater coverage area
Message received by AP,
AP forward the message to client B
802.11b/g
802.11a
Client B received the message
Start to send message to AP
Faster data transfer
Wireless client B
Wireless client A
Client A want to send message to client B

CSMA/CA

→ un équipement près du point d'accès disposera d'un bon débit, nominalement 11 Mbit/s, puis, lorsqu'il s'éloigne, celui-ci passe à 5,5 Mbit/s, 2 Mbit/s, et finalement 1 Mbit/s à mesure que le signal s'affaiblit et se dégrade.



→ Cette anomalie, inhérente au protocole d'accès au médium CSMA/CA défini dans la norme IEEE 802.11.

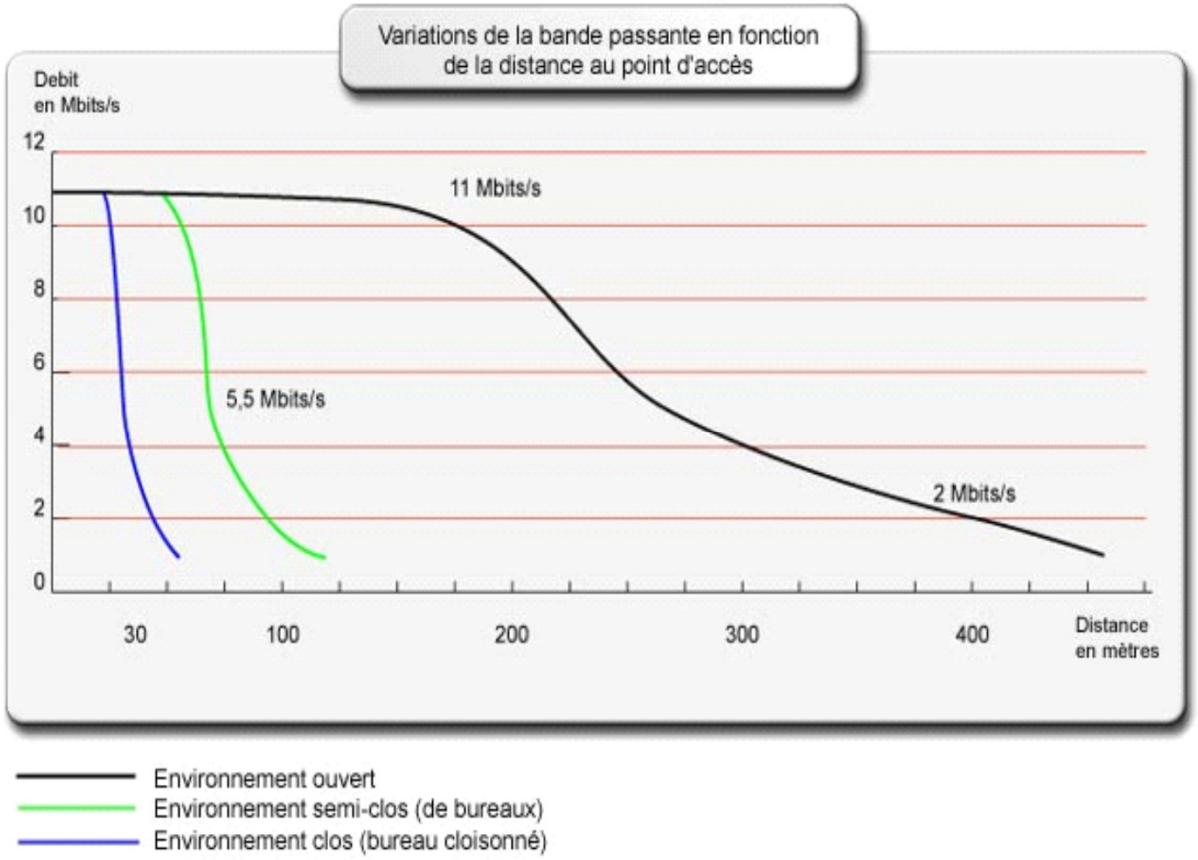
CSMA/CA

- Dans le cas hertzien, le protocole d'accès permet d'éviter la collision en obligeant les deux stations à attendre un temps différent avant de transmettre.

- Comme la différence entre les deux temps d'attente est supérieure au temps de propagation sur le support de transmission, la station qui a le temps d'attente le plus long trouve le support physique déjà occupé et évite ainsi la collision.

- Cette nouvelle technique s'appelle le CSMA/CA (Collision Avoidance).

La portée et les débits du WI-FI



Le débit du WLAN dépend de plusieurs facteurs, dont :

- Le nombre d'utilisateurs
- La portée des micro-cellules
- Les interférences
- La propagation multiple
- Le type de matériel
- Les protocoles utilisés
- Les règles d'accès.

Précaution à prendre:

Lors de l'installation des points d'accès WLAN :

- sélectionner pour chaque point d'accès l'endroit le plus approprié pour couvrir la zone choisie, c'est-à-dire choisir l'emplacement qui procure à tous les utilisateurs potentiels une connexion qui correspond à la qualité de service désirée en limitant toute exposition inutile.

- ne pas installer plus de points d'accès qu'il n'en faut (pour des questions de brouillages réciproques) : **un point d'accès est adapté pour une dizaine de personnes**.

- Positionner les points d'accès, de préférence, en hauteur (plus haut que la hauteur de la tête : 2,10m par exemple), pour limiter l'exposition des personnes et pour augmenter le rayon de couverture.

Fréquences Radio

Radio AM
0.55 ~ 1.6 MHz

Radio FM
88 ~ 108 MHz

Wireless LAN(802.11b/g) (802.11a)
2.40 ~ 2.4835 GHz 5.150 ~ 5.725MHz

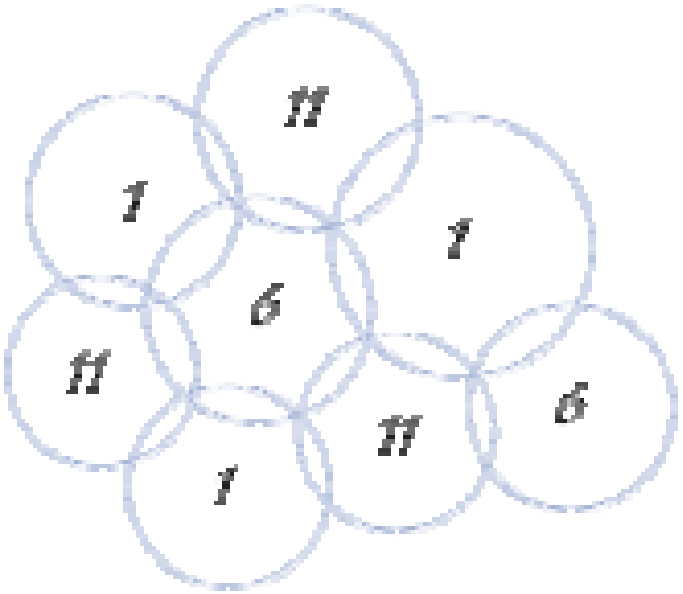
Four à Micro-ondes
2.45 GHz

Téléphones mobile GPRS
2.5 Ghz

Exemples d'atténuation du signal

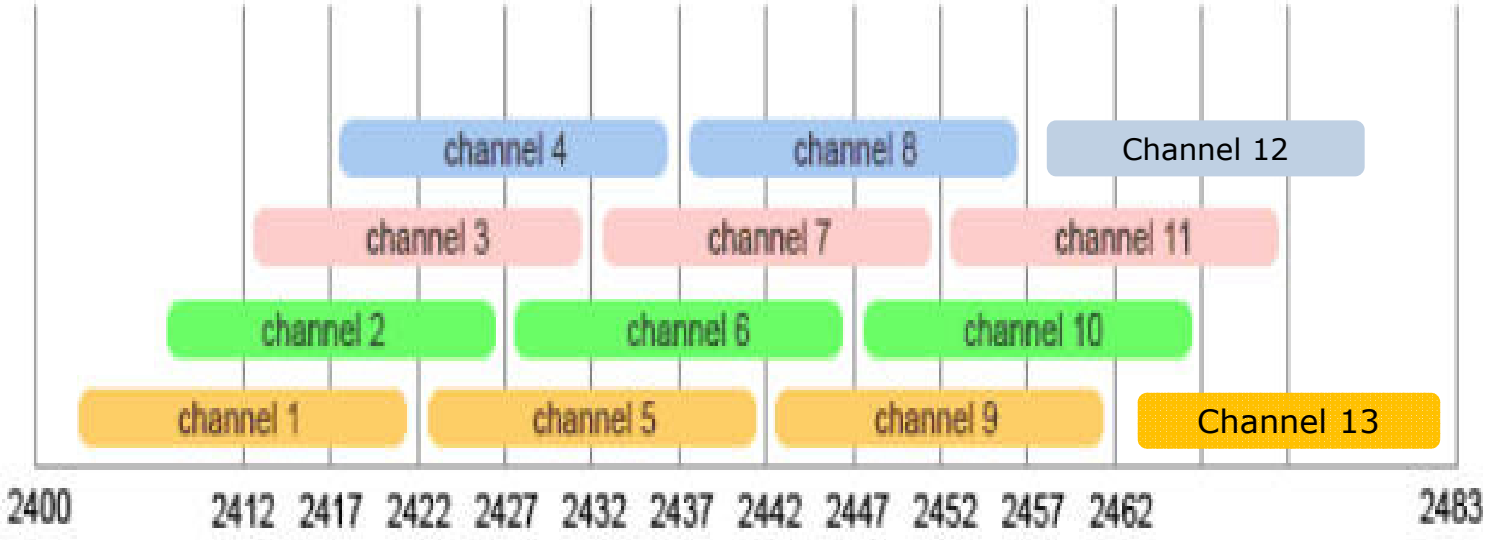
Matériaux	Affaiblissement	Exemples
Air	Aucun	Espace ouvert, cour intérieure
Bois	Faible	Porte, plancher, cloison
Plastique	Faible	Cloison
Verre	Faible	Vitres non teintées
Verre teinté	Moyen	Vitres teintées
Eau	Moyen	Aquarium, fontaine
Êtres vivants	Moyen	Foule, animaux, humains, végétation
Briques	Moyen	Murs
Plâtre	Moyen	Cloisons
Céramique	Élevé	Carrelage
Papier	Élevé	Rouleaux de papier
Béton	Élevé	Murs porteurs, étages, piliers
Verre blindé	Élevé	Vitres pare-balles
Métal	Très élevé	Béton armé, miroirs, armoire métallique, cage d'ascenseur

Channel	Frequency
1	2412 MHz
2	2417 MHz
3	2422 MHz
4	2427 MHz
5	2432 MHz
6	2437 MHz
7	2442 MHz
8	2447 MHz
9	2452 MHz
10	2457 MHz
11	2462 MHz
12	2467 MHz
13	2472 MHz

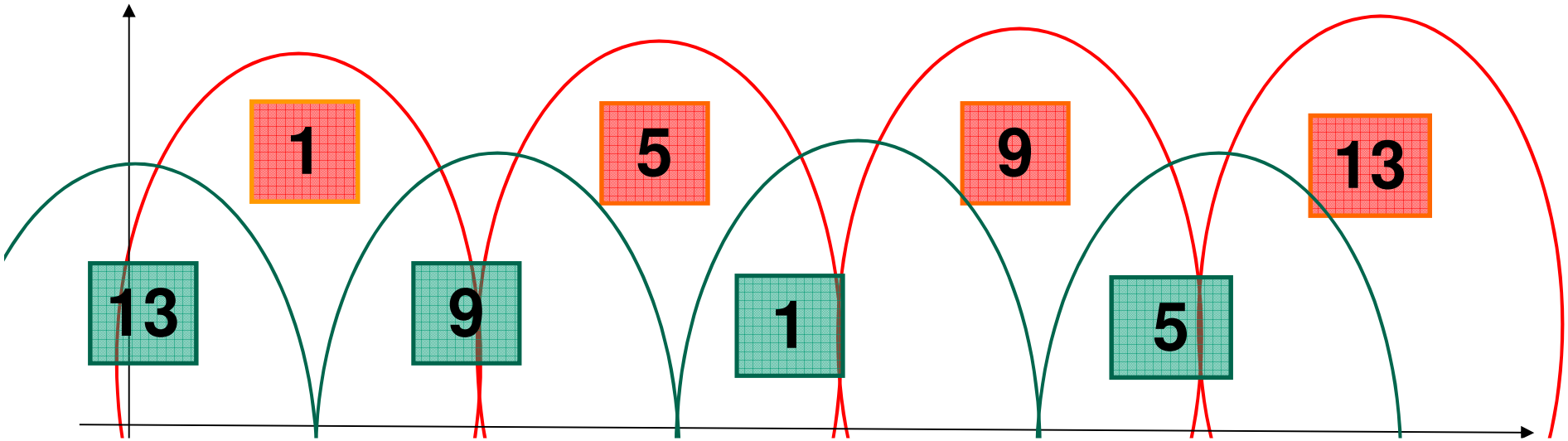


→ Plusieurs points d'accès peuvent être installés pour couvrir une large distance ou augmenter la bande passante, mais les points d'accès dont la couverture se chevauche doivent utiliser des canaux non-overlapping différents.

802.11b/g : Canaux non-overlappés



→ Trois points d'accès suffisent par zone de couverture (capacité surfacique maximale : 33 Mbit/s), en utilisant un plan de fréquence approprié (**1/6/11**, **2/7/12**, **3/8/13**, **5/10**).


1
5
9
13
13
9
1
5

La réglementation française

www.arcep.fr

Questions - Réponses / Les questions les plus fréquentes

Dois-je déclarer mon activité à l'ARCEP ?

➢ Seuls les réseaux ouverts au public doivent faire l'objet d'une déclaration à l'ARCEP.

Les réseaux utilisant des fréquences libres d'usage		
Réseaux ouverts au public		Réseaux n'étant pas ouverts au public
Réseaux ouverts au public	Réseaux internes ouverts au public (ex : cybercafés, hôtels ou toute offre de service à partir d'une borne connectée à un réseau déjà déclaré)	Réseaux indépendants (ex : réseau d'entreprises) Réseaux privés
Doivent se déclarer à l'ARCEP	Ne doivent pas se déclarer à l'ARCEP	

La réglementation française pour la bande des 2.4GHz

Pour les WLANs :

- En métropole, les canaux disponibles pour des applications Wifi ? (Mise à jour le 6 juillet 2007)

- Dans la bande 2,4 GHz : Les canaux utilisables sont les canaux 1 à 13.
  La limitation de puissance isotrope rayonnée équivalente autorisée est de:
  - 100 mW dans les canaux 1 à 9
  - 10 mW dans les canaux 10 à 13.

- Dans les bandes des 5GHz (5150-5350 MHz, ouverte uniquement en usages indoor et 5470-5725 MHz) : aucune canalisation n'est prévue au niveau européen, dans le respect des principes de neutralité technologique.

LES EQUIPEMENTS WiFi :

- **CARTE RESEAU PCI**

→ S'installe sur le port PCI d'une unité centrale d'un ordinateur

- **CARTE RESEAU PCMCIA**

→ Se connecte dans le port PCMCIA d'un ordinateur portable

- **CLE USB**

→ Se branche sur le port USB d'un ordinateur

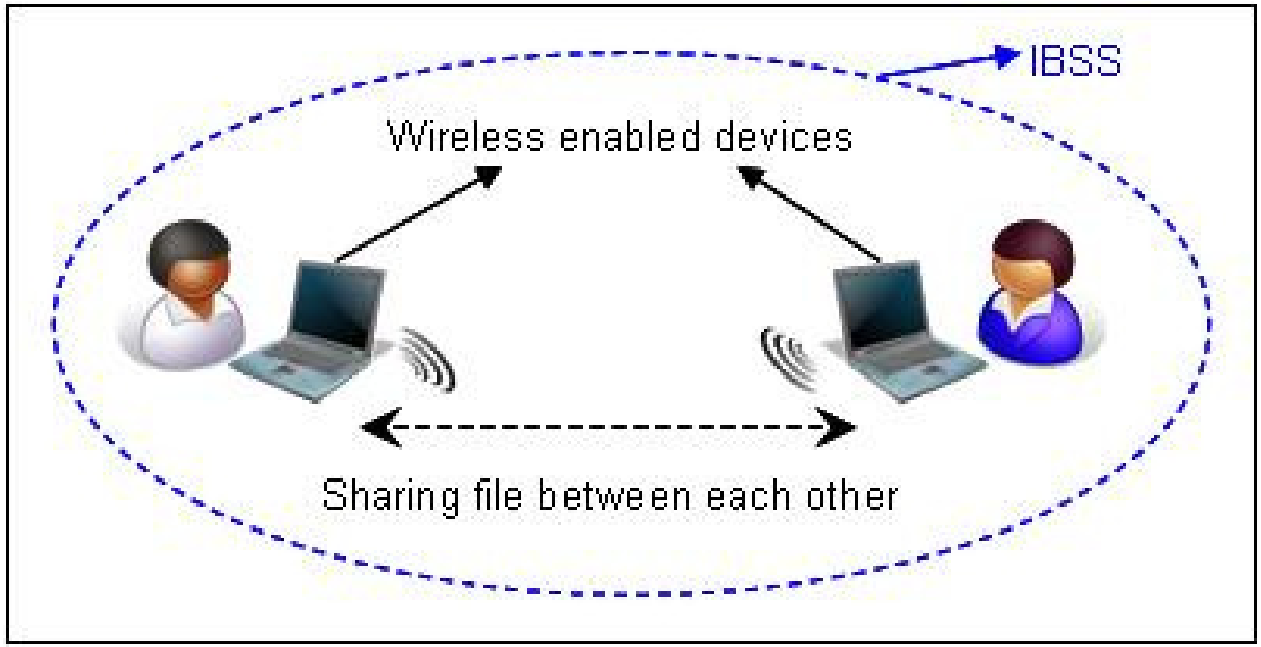
- **POINT D'ACCES**

→ Équipement central d'interconnexion des équipements WiFi

- **Antenne**

Le mode « ad-hoc » :

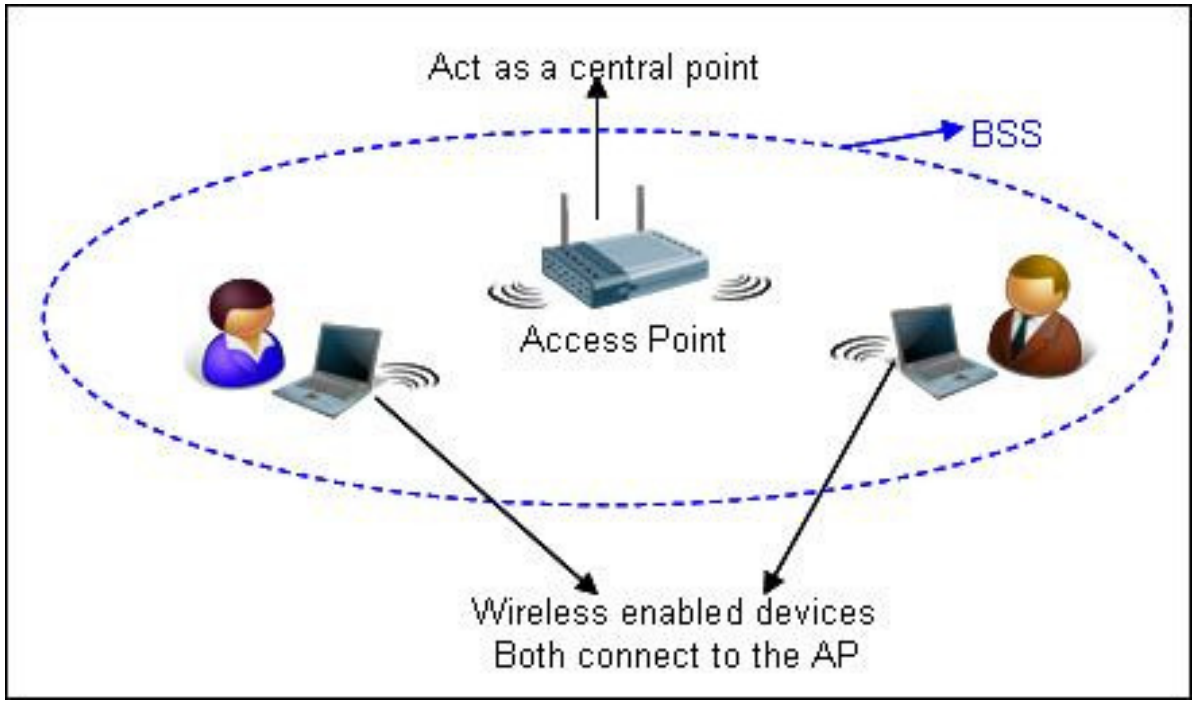
Le mode « **Ad-Hoc** » est un mode de fonctionnement qui permet de connecter directement les ordinateurs équipés d'une carte Wi-Fi, sans utiliser un matériel tiers, tel qu'un point d'accès. Ce mode est idéal pour interconnecter rapidement des machines entre elles sans matériel supplémentaire.



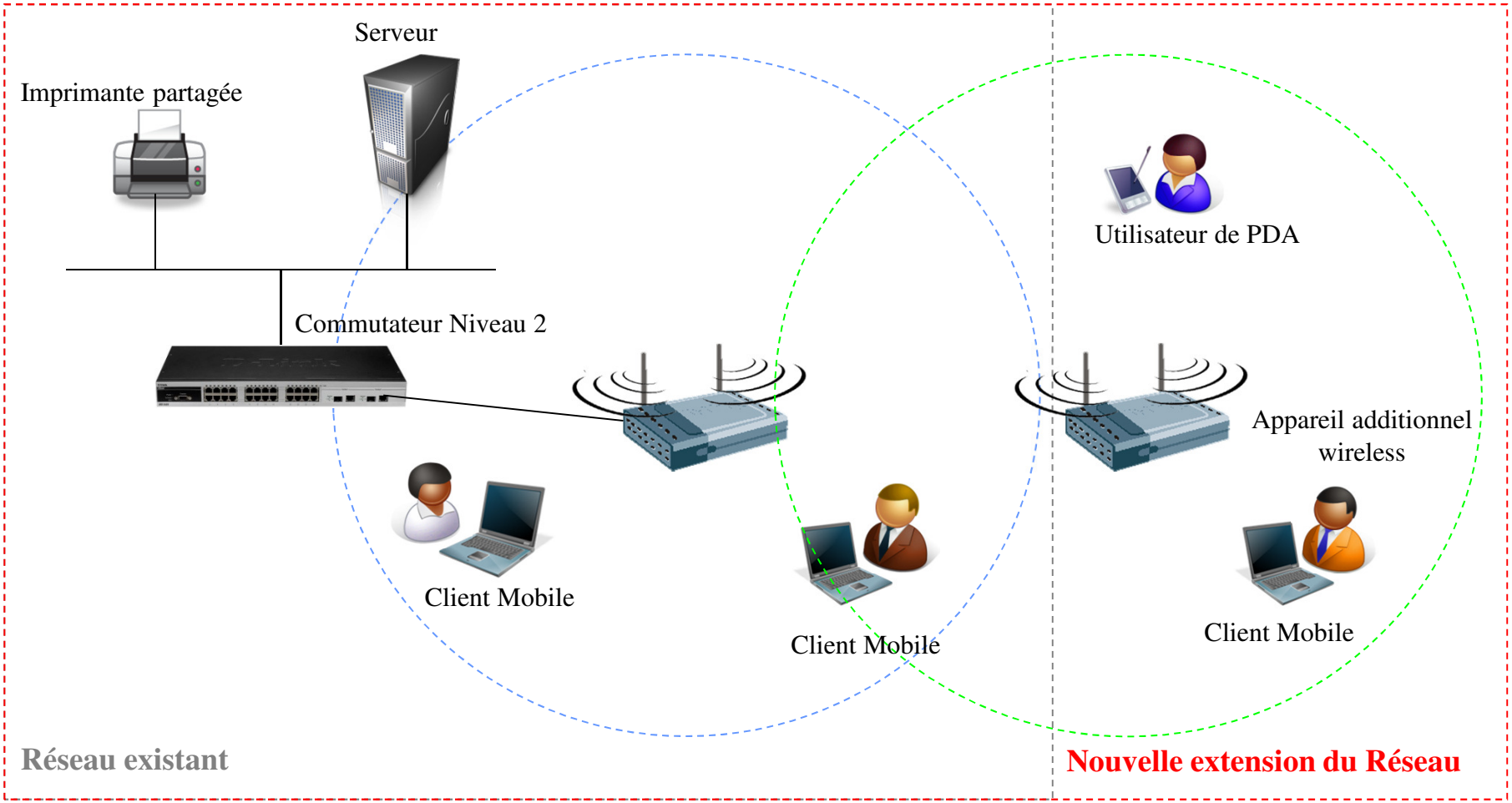
Mode Infrastructure (1/2)

Le mode « infrastructure » :

Le mode Infrastructure est un mode de fonctionnement qui permet de connecter les ordinateurs équipés d'une carte Wi-Fi entre eux via un ou plusieurs Point d'accès (AP) qui agissent comme des concentrateurs (exemple : répéteur ou commutateur en réseau Ethernet).

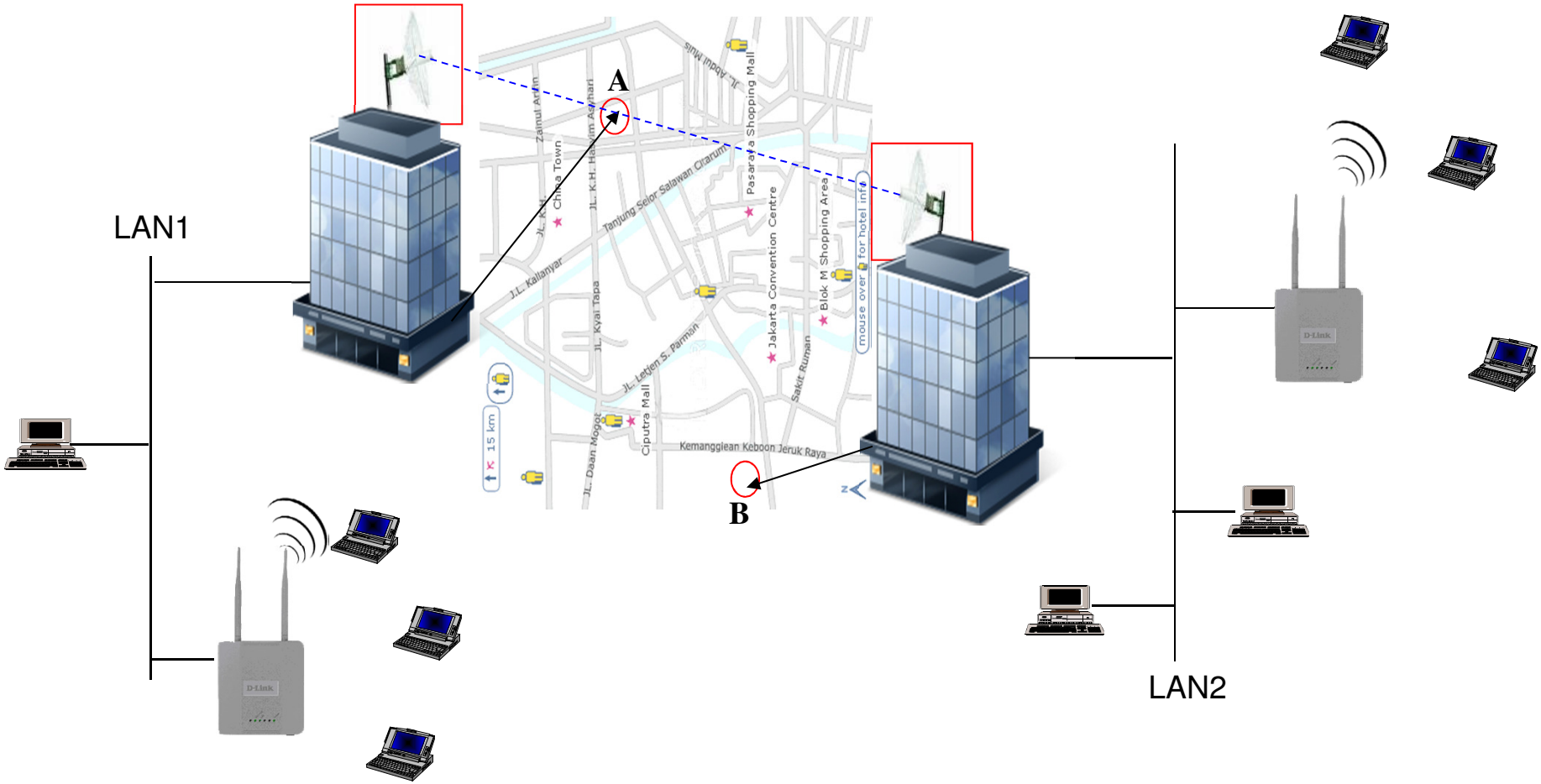


Mode Infrastructure (2/2)



Pont Wireless ou mode WDS

- Si le point d' accés le permet…



Sécurité: vulnérabilités du sans fil

- Si un réseau WIreless présente de nombreux avantages, gardons à l'esprit qu'un réseau mal configuré constitue une porte d'entrée vers vos données personnelles et/ou professionnelles.

- Un réseau sans fil peut-il être sûr à 100 % ?

- Que valent les différentes sécurités ?

- Quelles sont les règles élémentaires à respecter pour bien protéger son réseau ?

- Nous apporterons une réponse à ces nombreuses questions en passant en revue les différentes sécurités existantes (filtrage MAC, WEP, WPA).

La Sécurité: vulnérabilités du sans fil

- **Vulnérabilité de la technologie :** les données sont diffusées dans les airs. Le réseau peut diffuser au-delà de la zone concernée. De plus, le sans fil est sensible au brouillage.

- **Vulnérabilité du protocole :** de base, l'identifiant du réseau (SSID) n'est pas chiffré et on peut donc facilement l'intercepter. De plus, la méthode d' encryption WEP présente quelques faiblesses.

Wired Equivalent Privacy

- Le **Wired Equivalent Privacy** (abrégé **WEP**) est un Protocole obsolète pour sécuriser les réseaux sans-fil de type WI-FI.

- Les réseaux sans-fil diffusant les messages échangés par ondes radioélectriques, sont particulièrement sensibles aux écoutes clandestines.

- Le WEP tient son nom du fait qu'il devait fournir aux réseaux sans-fils une confidentialité comparable à celle d'un Réseau local filaire classique.

Sécurité WEP (niveau de sécurité : faible)

Nombre de caractères à saisir si la clef est stockée au format texte (ASCII) :

Longueur totale de la clef	**Longueur des IV**	**Longueur utile de la clef**	Nombre de caractères à saisir
64 bits	24 bits	40 bits (64-24)	**5** (40/8)
128 bits	24 bits	104bits (128-24)	**13** (104/8)
256 bits	24 bits	232 bits (256-24)	**29** (232/8)
512 bits	24 bits	488 bits (512-24)	**61** (488/8)

Nombre de caractères à saisir si la clef est stockée au format Hexadécimal :

Longueur totale de la clef	**Longueur des IV**	**Longueur utile de la clef**	Nombre de caractères à saisir
64 bits	24 bits	40 bits (64-24)	**10** (40/4)
128 bits	24 bits	104bits (128-24)	**26** (104/4)
256 bits	24 bits	232 bits (256-24)	**58** (232/4)
512 bits	24 bits	488 bits (512-24)	**122** (488/4)

Casser un cryptage WEP ?

- De nombreux programmes permettent de briser une clef WEP.
Le plus célèbre d'entre eux comprend cinq outils permettant de mettre à l'épreuve un réseau Wi-Fi.

- Avec de telles applications, la pénétration des réseaux sans fil n'est plus réservée aux seuls experts.

- Le WEP n’est plus suffisement sécurisé, la clef transitant dans la trame wireless, et est remplacé par le WPA

Sécurité 802.11i & le WPA

- Le but de **IEEE 802.11i** est d'améliorer les vulnérabilités de WEP tout en permettant la compatibilité avec les équipements existants. Le standard inclut de nouveaux protocoles pour l'authentification et l'encryptage.

- Contenus :

  - Pour l'encryptage et l'intégrité des données :
    - ✓ Il définit WEP, TKIP, et AES-(CCM ou OCB), MIC
  - Pour la sécurité :
    - ✓ 802.11i définit **802.1x** et d'autres fonctions de sécurité.

WiFi Protected Access - WPA

- WI-FI Protected Access (WPA et WPA2) est un mécanisme pour sécuriser les réseaux sans-fil de type WIFI.

- Ils ont été créés en réponse aux nombreuses et sévères faiblesses que des chercheurs ont trouvées dans le mécanisme précédent, le WEP.

- WPA respecte la majorité de la norme IEEE 802.11i et a été prévu comme une solution intermédiaire pour remplacer le WEP en attendant que la norme 802.11i soit terminée.

Sécurité WPA et WPA2 (niveau de sécurité : fort)

- Le WPA2 prend la relève et apporte quelques améliorations. L'implémentation du cryptage AES (Advanced Encryption Standard) améliore en effet le niveau de sécurité comparé à TKIP alors que les temps de latence au niveau de l'échange des clés ont été réduits.

- Si vous utilisez une clef « exotique », cette méthode de cryptage donnera beaucoup de fil à retordre aux personnes qui désireront s'introduire sur votre réseau sans fil.

Remarque : sur Windows XP Service Pack 2, le WPA2 n'est pas supporté nativement. Si vous utilisez cette sécurité, pensez à télécharger le patch de mise à jour sur le site de Microsoft

WiFi Protected Access - WPA

- WPA : WI-FI Protected Access = Wep avec clef dynamique
- Les clefs Wep sont modifiés cycliquement tous les 10,000 paquets
- Configuration dynamique
- Compatible IEEE802.1x (Serveur Radius)
- Tous nos produits supportent le WPA, ou le supporteront via une mise à jour firmware/Drivers.

Impact du cryptage sur les performances

- Théoriquement, le cryptage des données à un impact négatif sur les performances d'un réseau Wi-Fi.

- Dans la pratique, on constate que le temps de transfert d'un fichier de 310 Mo est quasi identique quelle que soit la configuration choisie.

- Avec ou sans cryptage, en WEP ou en WPA, le temps de copie varie dans les faits de façon presque négligeable comme en attestent nos mesures ci-dessous, des mesures effectuées en WiFi 802.11g :

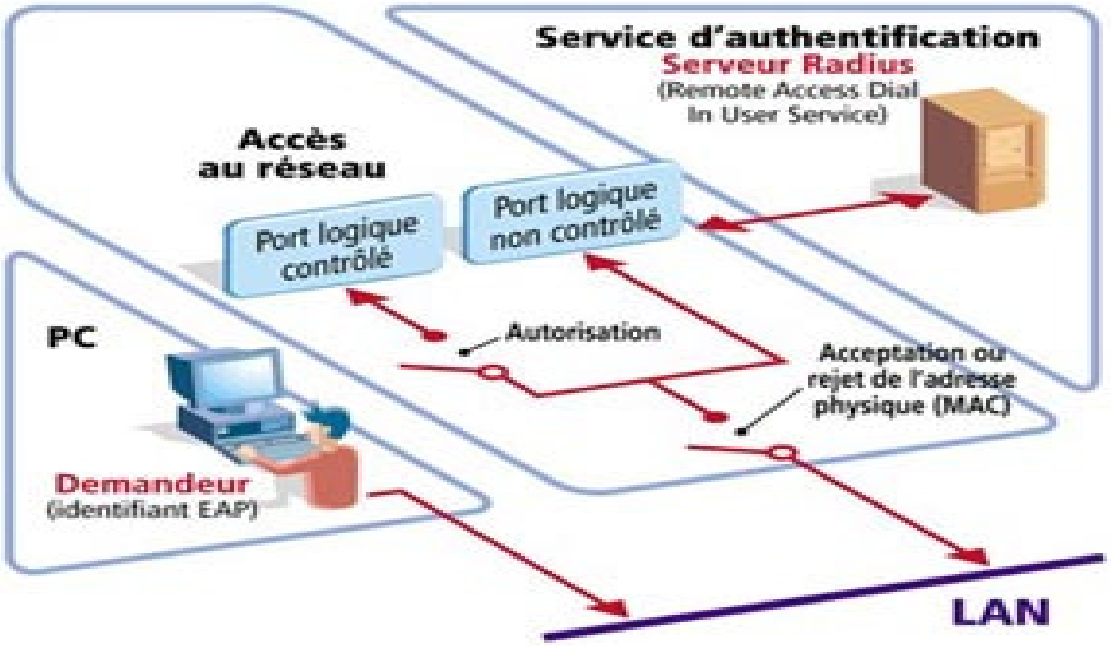
Sécurité	**Durée du transfert**
Sans cryptage	2 min 09
WEP 128 bits	2 min 16
WPA-PSK	2 min 14

Authentification 802.1x

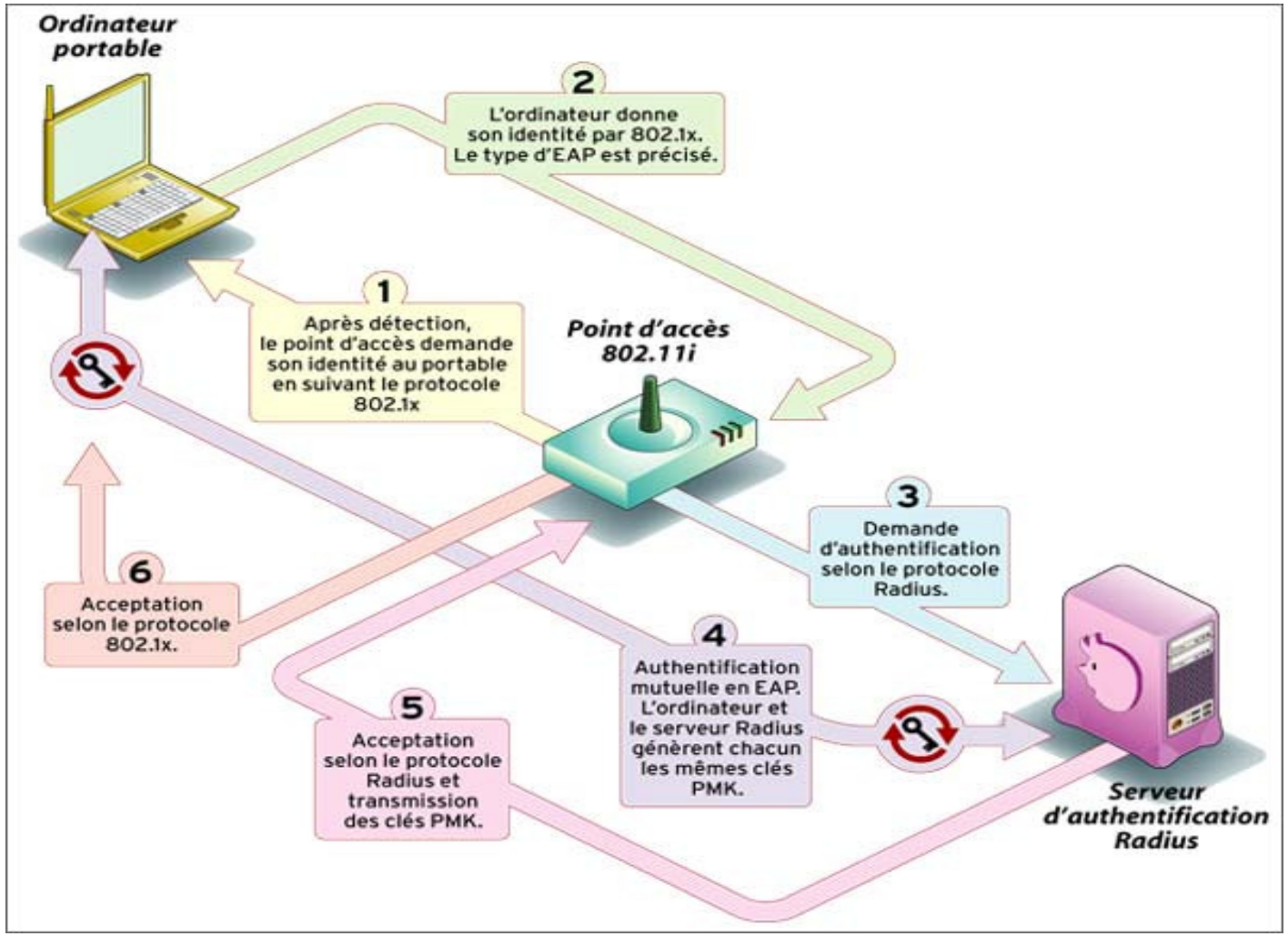
• 802. 1x transforme chaque port Ethernet d'un commutateur en intermédiaire entre l'utilisateur et le serveur Radius chargé de l'authentification.

• Deux ports logiques sont associés à l'adresse physique.

• Le premier, non contrôlé, achemine la requête du demandeur. Une fois celui-ci authentifié, le trafic passera par le second, dit contrôlé, configuré dynamiquement selon les droits de l'utilisateur.



Authentification 802.1x

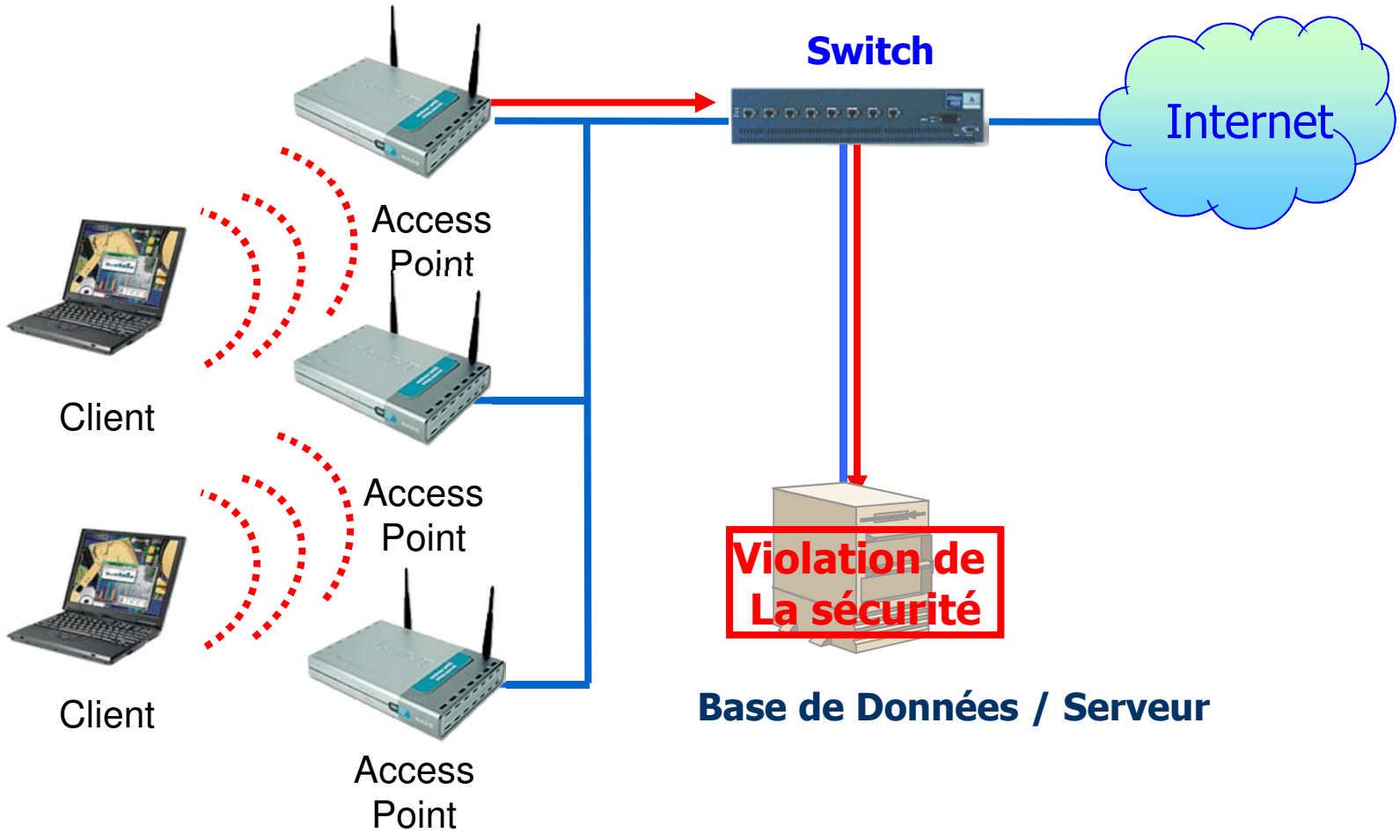


D-Link
Building Networks for People

Solutions minimales pour rendre le réseau sans fil plus sûr

- **Sécuriser les bornes d'accès par :**
  - la suppression de la configuration par défaut du point d'accès en modifiant l'identifiant réseau (SSID) et la clé Wep par défaut
  - la suppression de la diffusion du SSID
  - la protection des services d'administration disponibles sur l'interface sans fil en changeant le mot de passe
  - la mise en place du filtrage des adresses MAC ayant le droit de communiquer avec la borne
- **Limiter la couverture d'émission du réseau par :**
  - la gestion de la puissance d'émission du point d'accès si celui-ci le permet.

Configuration Classique



Power Over Ethernet alias POE

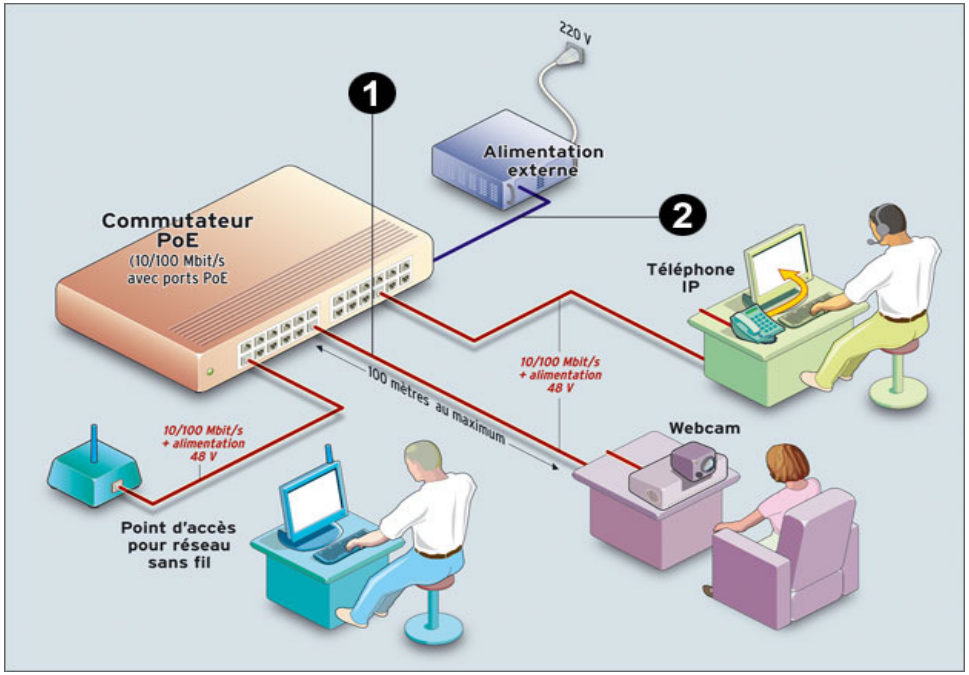
→un seul câble pour les données et l'alimentation électrique.

- Le groupe de travail **IEEE 802.3af** propose d'alimenter électriquement les équipements Ethernet par le câble Ethernet lui-même.
- La puissance peut être fournie sur des paires de données (1/2 comme – et 3/6 comme +) comme sur des paires détachées (4/5 comme + et 7/8 comme–) de câblage standard CAT-5.
- Le Power over Ethernet(PoE) fait disparaître les câbles d'alimentation électrique, ce qui réduit les coûts.

Power Over Ethernet alias POE

• Les équipements peuvent être aussi bien des commutateurs du réseau que des points d'accès Wifi ou d'autres équipements réseau qui se branchent sur une prise Ethernet.

Power Over Ethernet alias POE



1 - Chacun des équipements télé alimentés doit être relié au commutateur PoE. Ils doivent se **situer à moins de 100 mètres** du commutateur. La tension délivrée est de **48 v.**

2- La puissance varie en fonction du commutateur. Au maximum, elle est de **15,4 watts**. Pour délivrer une telle puissance sur 24 ports, il faut souvent ajouter une alimentation externe au commutateur.

Les applications WLAN : A l'intérieur des bureaux

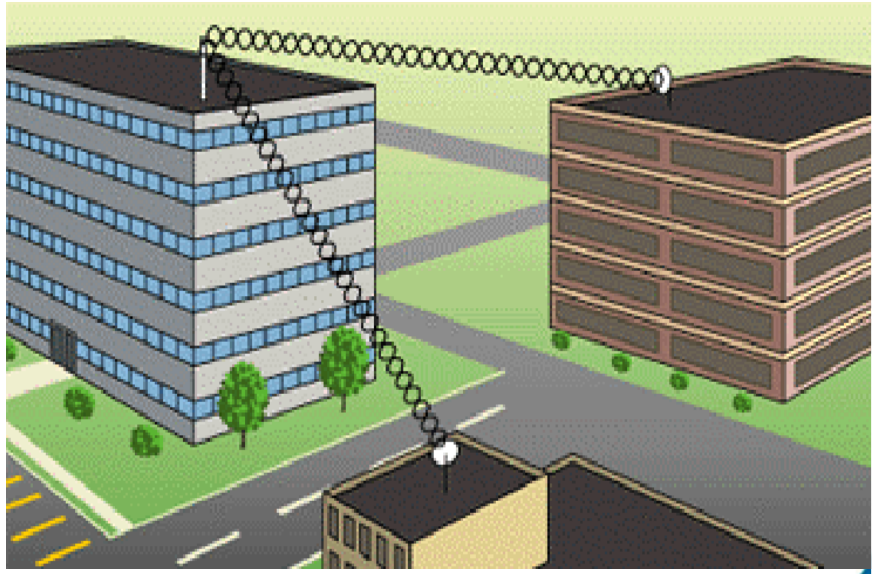
- Mobilité réseau :
  - accès constant aux données de l'entreprise
- Complément du réseau filaire existant
- Accès réseau là où les câbles ne peuvent pas passer
- Installation de réseau temporaire
- Déploiement réseau rapide et économique

- Connexion bâtiment-à-bâtiment :

  → Elimine les coûts récurrents d'une ligne spécialisée,les barrières physiques et les délais d'installation.

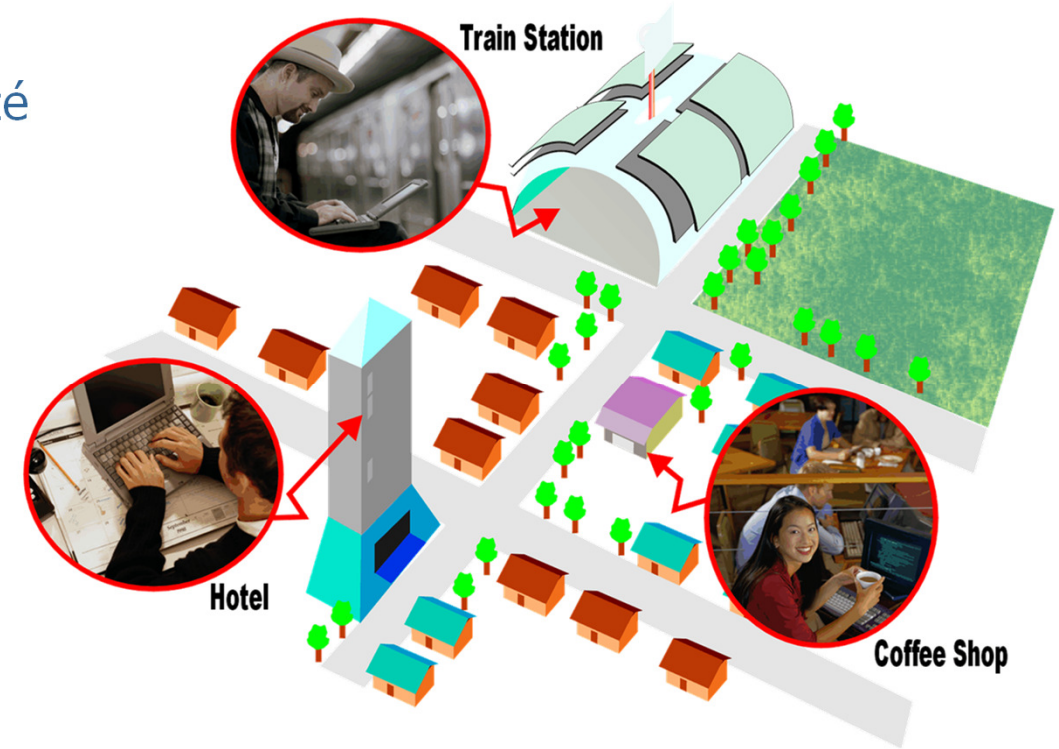
  → Facile à déployer

  → Utilisation gratuite



Les applications WLAN : Hotspots

- Aires d'accès Internet Haut Débit dans les lieux publics : les aéroports, les gares, les hôtels, les centres de conventions, ...
- Partage d'accès haut débit par satellite
- Coût d'implantation limité
- Taux de transmission rapide



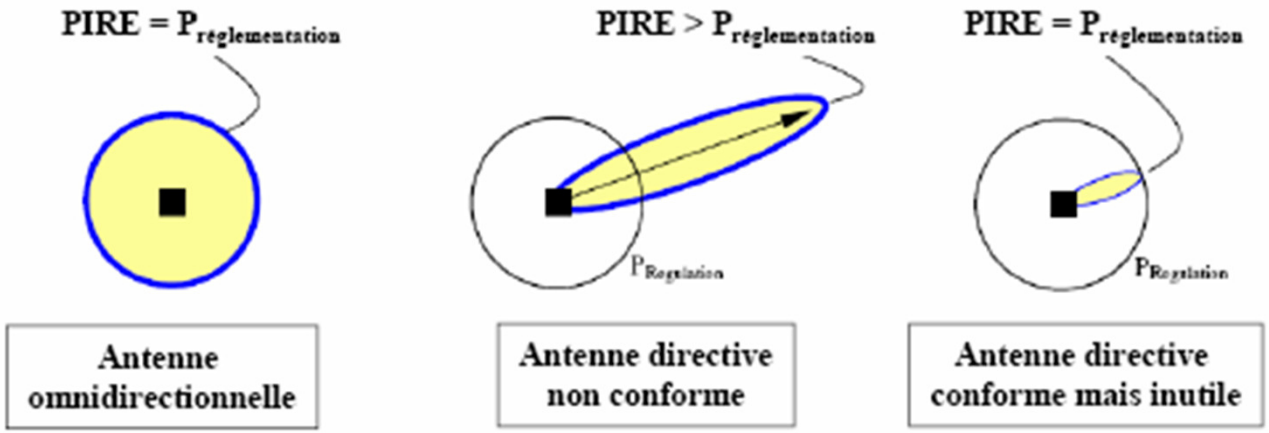
Qu’est ce que la P.i.r.e ?

- La P.i.r.e est la **puissance isotrope rayonnée équivalente** d’une antenne.

- Elle est exprimée en Watt.

- Elle est égale au produit de la puissance fournie à l’antenne d’émission par le **gain** de l'antenne.

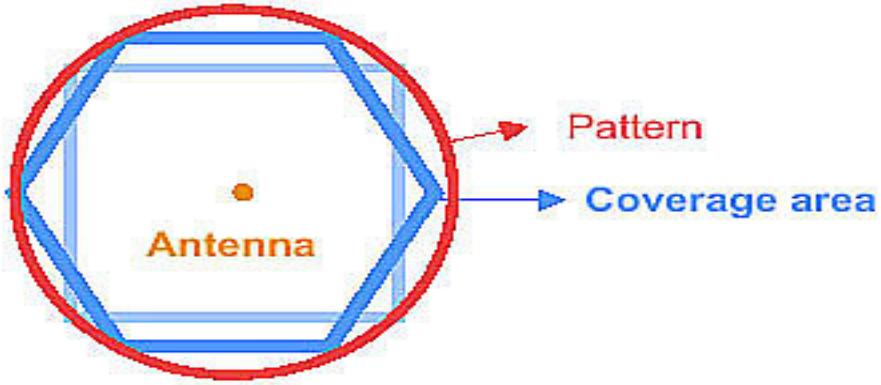
- Les graphiques suivant illustrent les situations de conformité et de non conformité à la P.i.r.e.



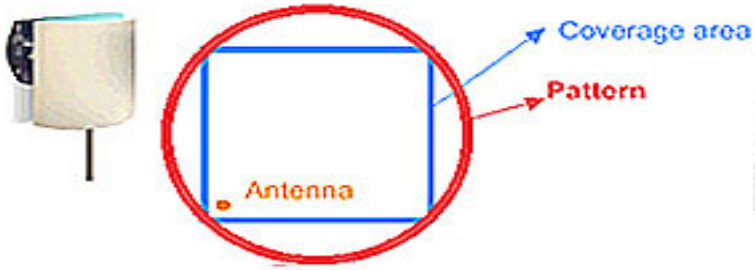
Types d'antennes

How to use antenna

Omni antenna



Directional antenna



D-Link
Building Networks for People

Antennes

Product Code	Image	Connector Type	dBi Gain	Indoor/Outdoor	Omni/Directional	Horizontal/Vertical Angle	Typical Distance* M 1 Mbps	11Mbps
PORTABLE ANTENNAS								
ANT24-0400**		MMCX	4	Indoor	Omni	H360°/V40°	40	15
DWL-M60AT		SMA - Female	6	Indoor	Directional	H80°/V80°	60	25
DWL-50AT		SMA - Female	5	Indoor	Omni	Omni	60	25
DWL-R60AT		SMA - Female	6	Indoor	Directional	H80°/V75°	60	25
WALL /CEILING MOUNT ANTENNAS								
ANT24-0401		SMA - Female	4	Indoor	Omni	H360°/V120°	40	15
ANT24-0500		N - Female***	5	Both	Omni	H360°/V30°	40	15
ANT24-1200		SMA - Female***	12	Indoor	Directional	H80°/V23°	1 Km	300
MID GAIN ANTENNAS								
ANT24-0800		N - Female***	8	Outdoor	Omni	H360°/V15°	800	200
ANT24-0801		N - Female***	8.5	Both	Directional	H70°/V70°	800	200
ANT24-1201		N - Female***	12	Indoor	Directional	H50°/V50°	1 Km	300
HIGH GAIN ANTENNAS								
ANT24-1400		N - Female***	14	Both	Directional	H30°/V30°	1 Km	300
ANT24-1800		N - Female***	18	Both	Directional	H15°/V15°	1.2 Km	300
ANT24-1801		N - Female***	18	Outdoor	Directional	H15°/V15°	1.2 Km	300
Product Code	Image	Connector Type	dBi Gain	Indoor/Outdoor	Omni/Directional	Horizontal/Vertical Angle	1 Mbps Typical Distance* M	11Mbps

*Distances quoted are for reference only and will vary dependent on the environment, ** Only for DWL-660 adapter, ***All antennas with N - female connectors will come supplied with a N – female to SMA – female pigtail. Use of high gain antennas need careful planning to conform with EU regulations and extra consideration to avoid causing a potential health hazard. Products with SMA connector – DWL-520+, DWL-G520, DWL-900AP+, DWL-1000AP+, DWL-2000, DI-614+, DI-714P+, DI-624

D-Link
Building Networks for People

MERCI